

Assunto: Política de Segurança da Informação	Versão: 1.5	Publicado em: 01/08/2023
Autores: Segurança da Informação, TI e Administração	Classificação: Restrito	Última revisão: 30/06/2026

1. OBJETIVO

A Política de Segurança da Informação dá direcionamento e suporte para proteção de informações, rege o uso de todos os sistemas eletrônicos, a fim de garantir as melhores práticas de utilização e de segurança, define as responsabilidades de cada área, ajuda a implementar controles que reduzem riscos e vulnerabilidades, para melhorar a segurança das informações no nosso ambiente de trabalho e visa também garantir a conformidade com as legislações vigentes de proteção de dados (como a LGPD) e regulamentações do setor de saúde aplicáveis

A Segurança da Informação é uma proteção a uma grande variedade de ameaças. Esta proteção é sob os ativos, à continuidade de negócios, minimiza os riscos, melhora o retorno aos investimentos e oportunidades de negócios.

2. ABRANGÊNCIA

Todos os colaboradores e prestadores de Serviços com acesso aos Recursos de TI da Salud Valor.

3. CONCEITOS IMPORTANTES

A informação é um ativo que, como outros ativos comerciais importantes, é essencial para o negócio de uma organização e, conseqüentemente, precisa ser adequadamente protegido. Isto é especialmente importante no ambiente empresarial cada vez mais interconectado. Como resultado desta crescente interconectividade, a informação está agora exposta a um número crescente e a uma variedade maior de ameaças e vulnerabilidades.

Os principais pontos para a proteção e segurança da informação pautado neste documento são:

- **Integridade da informação:** garantir o sigilo da informação e que esta seja mantida em seu estado original, protegendo de alterações;
- **Confidencialidade:** proteger e garantir que a informação seja acessada somente por pessoas a autorizadas;
- **Disponibilidade:** permitir e garantir aos usuários autorizados acesso à informação e aos ativos correspondentes sempre que necessário.
- **Ativo:** Qualquer coisa que tenha valor para a organização e que necessita de algum tipo de proteção.
- **Ameaça:** Evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas.
- **Vulnerabilidade:** Ausência de um mecanismo de proteção ou falhas em um mecanismo de proteção existente. São as vulnerabilidades que permitem que uma ou mais ameaças se concretizem.

- **Incidente:** São as ameaças que se concretizam.
- **Impacto:** Tamanho do prejuízo, medido através de propriedades mensuráveis ou abstratas, que a concretização de uma determinada ameaça causará.
- **Risco:** Medida que indica a probabilidade de uma determinada ameaça se concretizar, combinada com os impactos que ela trará. É a principal métrica gerencial de Segurança da Informação. Quanto maior a probabilidade de uma determinada ameaça ocorrer e o impacto que ela trará, maior será o risco associado a este incidente.
- **Responsável pela Informação:** O Responsável da informação é aquele que, de alguma forma, zela pelo armazenamento e preservação de informações que não lhe pertencem, mas estão sob sua custódia. Os custodiantes são responsáveis pela administração de banco de dados, servidores de arquivos ou cofres para armazenamento de ativos valiosos.

4. RESPONSABILIDADES

4.1. EQUIPE DE TI

- Responsável por configurar os recursos de TI de acordo com as Políticas corporativas;
- Avaliar os incidentes de segurança e propor ações corretivas;
- Avaliar os riscos identificados, propor planos de mitigação tecnológica e apoiar os proprietários dos riscos na tomada de decisão."
- Responsável por garantir a correta utilização do uso dos recursos de TI;

4.2. SEGURANÇA DA INFORMAÇÃO

- Planejar, conduzir e acompanhar na conscientização dos colaboradores e terceiros a respeito da importância da cultura e Política de Segurança da Informação, mediante treinamentos, publicações e outros meios adequados.
- Deve manter a Política de Segurança da Informação atualizada e realizar revisões periódicas ou sempre que necessárias em função de um evento significativo, obter aprovação da administração bem como, comunicar a todos os colaboradores;
- Propor alterações nas versões da Política de Segurança da Informação e a inclusão, a eliminação ou a mudança de normas complementares;

4.3. ADMINISTRAÇÃO

- Decidir sobre as tratativas para riscos identificados.
- Definir as medidas cabíveis nos casos de descumprimento da Política de Segurança da Informação ou das Normas de Segurança da Informação complementares.
- Garantir a ciência de segurança da informação para todos os colaboradores e parceiros contratados na organização, bem como o termo de responsabilidade de ativos.
- Responsável por avisar a entrada de novos colaboradores.
- Responsável por avisar sobre as saídas de colaboradores, a fim de proceder com inabilitação em todos os sistemas.
- Atuar no processo de seleção e desligamento, observando as diretrizes de segurança da informação em tais processos.
- Aplicar o processo disciplinar para colaboradores que infringam regras de segurança da informação;

4.4. COLABORADORES SALUD VALOR

- Responsáveis por utilizar os recursos de TI de acordo com as normas definidas e comunicadas nesta política.
- Responsáveis por comunicar o responsável da área ou ao departamento de TI qualquer anomalia que contrarie as normas definidas nesta política.
- Responsáveis por classificar as informações (pública, restrita e confidencial) de sua área.

5. SISTEMA DE SEGURANÇA DA INFORMAÇÃO – SGSI

A Política de Segurança da Informação determina as regras gerais do Sistema de Gestão de Segurança da Informação da Salud Valor. O sistema de gestão de segurança da informação é o processo de implementação, operação, monitoramento, revisão, manutenção e melhoria contínua da segurança da informação na Salud Valor.

6. TREINAMENTO

A Salud Valor se responsabiliza em realizar treinamentos anuais com o objetivo de assegurar que os colaboradores e prestadores de serviços estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, estejam preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano. Comunicados tempestivos em função de nova ameaça ou risco relevantes deverão ser enviados, sempre que necessário, a fim de orientar a melhor forma de tratativa por parte dos colaboradores. As evidências da participação dos colaboradores nos treinamentos serão recolhidas mediante a realização formal.

7. PLANO DE GESTÃO DE RISCOS

Cumprindo seu compromisso com seus clientes, acionistas, colaboradores diretos e indiretos, a Salud Valor posiciona a gestão de riscos como um desafio indispensável para as operações do negócio bem como para manter e melhorar seu valor corporativo. Como os riscos têm se diversificado e aumentado, estes serão aceitos como oportunidades para a criação de um sistema de gerenciamento fortalecido, visando o crescimento e a prosperidade da organização.

8. CLASSIFICAÇÃO DA INFORMAÇÃO

Para assegurar a proteção adequada às informações da Salud Valor, somente profissionais autorizados devem possuir acesso às informações armazenadas pela Salud Valor, no nível de acesso e pela utilização de credenciais de acesso, conferidos pelo responsável da tecnologia da informação. Os níveis de acesso à informação se classificam da seguinte maneira:

- **Informações Públicas:** são informações de domínio público, que não contém quaisquer informações confidenciais ou sensíveis e podem ser acessados por qualquer pessoa, dentro ou fora da Instituição;
- **Informações Restrita:** são informações internas da Salud Valor, que contém informações relevantes e potencialmente confidenciais à Instituição, podendo ser acessados apenas pelos

integrantes da Instituição ou partes devidamente interessadas à informação, sob dever de confidencialidade;

- **Informações Confidenciais:** são documentos sigilosos da Instituição, que contém informações sensíveis e/ou confidenciais da Instituição ou de seus clientes, podendo ser acessados apenas pelos integrantes da Instituição instituídos ou partes devidamente interessadas e mapeadas, sob dever de confidencialidade e com as devidas credenciais de acesso.

9. TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Constitui incidente de Segurança da Informação qualquer ato que viole a confidencialidade, a integridade ou a disponibilidade dos ativos de informação, bem como qualquer acesso indevido aos sistemas ou à infraestrutura de tecnologia pertencentes à Salud Valor.

A área de tecnologia da informação deve conduzir o tratamento de incidentes de segurança, avaliar o risco, registrar as ações para remediação com os responsáveis e atuar em conjunto com outras áreas para a resolução do incidente, com transparência, imparcialidade, ética e sigilo.

Após o encerramento do incidente de segurança, a área de tecnologia da Informação deve informar a área administrativa conforme a matriz de criticidade e impacto definida no plano de resposta a incidentes. A área de administração deverá avaliar, e se aplicável, comunicar as áreas internas, que poderão definir sanções disciplinares aos envolvidos no incidente ou acionar autoridades legais.

As violações de segurança devem ser informadas imediatamente ao e-mail **ti@saludvalor.com.br**.

10. USO DE DISPOSITIVOS MÓVEIS

O colaborador deve zelar pela proteção do dispositivo móvel e das informações nele contidas, conforme:

- Não armazenar informações em dispositivos móveis (pen-drives, hard-drives, memory cards etc.), se não autorizados previamente;
- Em locais públicos deve-se manter o computador corporativo sempre próximo e à vista, para evitar furtos;
- Em viagem, o computador corporativo não deve ser colocado em carrinhos de bagagem dos aeroportos e nem despachado junto com a bagagem.
- É proibido o uso de serviços, ferramentas ou repositórios em nuvem não autorizados pela área de TI (Shadow IT) para o armazenamento, processamento ou transmissão de dados institucionais, de pacientes ou de clientes;
- Em hotéis o computador corporativo deve ser armazenado no cofre do quarto quando disponível;

Em caso de perda, roubo ou furto, deve-se notificar a área de tecnologia através do e-mail **ti@saludvalor.com.br** imediatamente.

11. PROTEÇÃO DAS INFORMAÇÕES DURANTE TRABALHO REMOTO

Os cuidados para o trabalho remoto devem ser redobrados. Os ativos utilizados em trabalho remoto devem ser protegidos minimamente pelos recursos de antivírus, possuir os mecanismos de atualização de sistemas e o local de trabalho deve garantir a confidencialidade das informações, apresentadas em tela ou falada.

A Salud Valor se compromete a manter e intensificar a conscientização a respeito da segurança da informação aos seus colaboradores, através de campanhas periódicas e treinamentos.

12. MESA LIMPA

Para reduzir os riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente, a Salud Valor considera a adoção de uma política de “mesa limpa”, visando o resguardo de informações constante em documentos e/ou impressos durante a ausência do funcionário do seu local e/ou estação de trabalho.

A política deve considerar as classificações de segurança da informação, os riscos correspondentes e os aspectos culturais da organização. Informações deixadas sobre as mesas de trabalho são passíveis de serem danificadas ou destruídas de diversas formas. O objetivo da política de “mesa limpa” é definir diretrizes que reduzam o risco de uma violação de segurança, fraudes e roubo de informações causadas por documentos que estão sendo deixados sozinhos nas instalações da empresa.

12.1. CONTROLE QUE DEVEM SER CONSIDERADOS

- Os papéis (relatórios) devem ser armazenados em armários trancados e/ou em outras formas de mobiliário de segurança, quando não estiverem em uso, especialmente fora do horário do expediente;
- Computadores pessoais e impressoras não devem ser deixados “logados” quando não houver usuário junto e devem estar protegidos por senhas e outros controles quando não estiverem sendo utilizados;
- Fotocopiadoras, quando utilizadas, devem ser protegidas contra uso não autorizado, durante e fora do horário de expediente;
- Informações sensíveis ou confidenciais, quando impressas, devem ser retiradas da impressora imediatamente;
- Utilize um protetor de tela que solicite uma senha para acesso;
- Descarte os itens referentes a informações dos clientes internos, externos ou de propriedade da empresa em locais designados seguros;
- Sempre limpar sua área de trabalho antes de ir para casa, garantindo adequada organização dos itens/objetos manipulados ou lembrando/anotando para quem você repassou para arquivar/guardar.
- As senhas não devem ser deixadas em notas adesivas coladas no computador ou embaixo dele, nem podem ser deixadas escritas em local acessível;
- Sua senha é pessoal e intransferível, por isso não repasse a ninguém.

13. REGRAS BÁSICAS DE COMPORTAMENTO

Conjunto de atitudes / comportamentos cuidadosos que devem ser observados – dentro e fora da organização – com foco na proteção das informações corporativas. É fundamental que o profissional seja reservado e cuidadoso nas suas opiniões, conversas, participações em eventos, principalmente quando em contato com o cliente e/ou a com terceiros. As diretrizes definidas nesta política visam conscientizar funcionários e colaboradores sobre as ameaças que rondam sua organização, bem como, orientá-los sobre condutas que ajudam a fortalecer o fator humano na proteção de ativos de sua organização.

14. TERMO DE CIÊNCIA DE SEGURANÇA DA INFORMAÇÃO

Todos os colaboradores devem assinar o termo de ciência do conjunto de políticas que compõem a segurança da informação no momento de ingresso na organização.

15. PROCESSO DISCIPLINAR

Todo colaborador deve cumprir as políticas, normas e procedimentos internos definidas pela Salud Valor, o descumprimento poderá acarretar processo disciplinar citado no **Contrato de Trabalho** onde são devidamente assinados.

Em nenhum momento será admitido, a qualquer usuário, invocar o desconhecimento das políticas, normas e procedimentos para justificar violações ou falta de cumprimento dela.

Todo e qualquer caso de descumprimento ou inobservância desta política estará sujeito à aplicação de sanções disciplinares, conforme normas internas existentes ou dispositivos constantes na CLT – Consolidação das Leis do Trabalho previstas no artigo 482, Lei de Proteção à Propriedade Intelectual, bem como demais leis vigentes.

16. HISTÓRICO DE VERSÕES

Esta política é revisada anualmente ou quando houver uma mudança significativa no escopo do Sistema de Gestão de Segurança da Informação da Salud Valor. O controle de revisão identifica número da versão, data, autor, as principais alterações e a aprovação da política.

Versão	Responsável	Data da Revisão	Alterações
1.0	Carlos Moreira	23/07/202	Versão inicial.
1.1	Carlos Moreira	24/09/202	Organização de papeis e responsabilidades.

1.2	Carlos Moreira	16/01/202	Inclusão dos termos de Mesa limpa e tela limpa, Riscos, regras de comportamento
1.3	Carlos Moreira	17/07/2025	Incluído as responsabilidades do time de Segurança da Informação no Item. 4.2. Removido o Item 4.5 - Gestão de Prestadores de serviço, item inserido na POC.SV14 - Política de Segurança da Informação para Fornecedores
1.4	Carlos Moreira	12/09/2025	Inclusão do texto de revisão anual do documento, Item 16
1.5	Carlos Moreira	30/06/2026	Melhoria de texto nos itens: 4, 5, 6, 7, 10,12.1, 13

17. APROVAÇÃO

VERSÃO	RESPONSÁVEL	DATA	APROVADOR
1.0	Carlos Moreira	21/08/2023	Daniela Floriano
1.1	Carlos Moreira	25/10/2024	Daniela Floriano
1.2	Carlos Moreira	13/05/2025	Daniela Floriano
1.3	Carlos Moreira	17/07/2025	Daniela Floriano
1.4	Carlos Moreira	12/09/2025	Daniela Floriano
1.5	Carlos Moreira	30/06/2026	Daniela Floriano